REMARKS

The Office Action of October 1, 2004, has been received and reviewed. Claims 1 through 30 are currently pending in the application. Claims 1 through 30 stand rejected. Applicant has amended claims 1, 3, 4, 7, 8, 13, 15, 16, 19 and 20, and respectfully requests reconsideration of the application as amended herein.

Claim Rejections Under 35 U.S.C. § 112(2)

Claims 19 and 20 stand rejected under 35 U.S.C. § 112, second paragraph, as being incomplete for omitting an essential element, i.e., steps reciting how a key is actually derived. Additionally, the Office asserts that there is no end result to both claims.

Initially, Applicant notes the assertion that claims 19 and 20 fail to set forth the subject matter that Applicant regards as the invention is properly considered only with respect to 35 U.S.C. § 112, first paragraph; it is irrelevant to compliance with the second paragraph of that section. The Office appears to be relying on the content of Applicant's specification to support its assertion, which is improper in this context. *See* MPEP 2172(II).

Nevertheless, without acquiescing to the basis for the present rejections, claim 19 has been amended to recite the limitation of "deriving the key by hashing at least one of the hint and the password," and claim 20 has been amended to recite the limitation of "deriving a key by hashing at least one of a password and a hint." Applicant submits that claims 19 and 20, as amended, are allowable under the provision of 35 U.S.C. § 112, second paragraph, and requests that the present rejections be withdrawn.

Claim Rejections Under 35 U.S.C. § 102(b)

Claims 1 through 18 and 21-30 stand rejected under 35 U.S.C. § 102(b) as being anticipated by Kaufman et al. (U.S. Patent No. 5,491,752). Applicant respectfully traverses this rejection, as hereinafter set forth.

A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference. *Verdegaal Brothers v. Union Oil Co. of California*, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). The identical invention must be shown in as complete detail as is contained in the claim. *Richardson v. Suzuki Motor Co.*, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989).

Turning to the cited reference, Kaufman et al. is directed to a system wherein a workstation 516 exchanges data with an authentication server 502 to obtain access to a network 500 and to establish a shared secret key for the protection of subsequent messages. The workstation 516 includes a token generator 520, and the server 502 includes a token generator 503.

In one embodiment described by Kaufman et al., workstation 516 computes a "transmission code" based upon a password and a token comprising a randomly generated number by using a first hashing algorithm (col. 9:31-43). A number of examples are provided for hashing equations, which may include hashing the password, concatenating the hashed password with the token, and then hashing the concatenation (col. 9:62 – col. 10:17). After computing the transmission code, the workstation sends it to the server 502 and the server 502 attempts to identify the token used in calculating the transmission code. The server 502 does this by utilizing a list of recent tokens provided by token generator 503 and a user password to try and duplicate the transmission code with the first hashing algorithm (col. 10:18-55).

If the calculations by the server 502 yield the received transmission code, it indicates that the token and password used to generate the transmission code are valid, and access to network 500 is granted (col. 11:12-24). Sever 502 then computes a "session code" by performing a second hashing algorithm, which may use a different one of the hashing equations described with respect to the first hashing algorithm, or may use the same equation but operate on the token and the password in a different order (col. 11:25-42). After computing the session code, the server encrypts a message using the session code as a secret key, and sends the message to workstation 516. Workstation 516 then calculates the session code and decrypts the message using the session code. Then the workstation 516 may use the message as a ticket to gain access to the desired system, or as a shared secret key to encrypt and decrypt subsequent communications with the desired system (col. 11:44-55).

Applicant respectfully submits that the above-described system of Kaufman et al. fails to disclose, either expressly or inherently, all of the elements recited in Claims 1-18 and 21-30.

Claim 1, as presently amended, recites "obtaining a hint" and "sending the hint to a client," claim 4 recites "sending the encrypted data and the hint to a server," and claim 8 recites "means for obtaining a hint" and "means for sending the hint to a client." Claims 13, 15 and 16, as presently amended recite "sending encrypted data and a hint corresponding to the encrypted data from a server to a client." Claim 21 recites "receiving a hint corresponding to data to be decrypted from a server." Claim 24 recites "generating an intermediate index from a hint received from a server," and claim 26 recites "means for receiving a hint corresponding to data to be decrypted from a server." Kaufman et al. fails to disclose the concept of sending a hint to a client or a server.

The Office considers the tokens described in Kaufman et al. as being analogous to a hint. None of the tokens, however, are described as being sent between workstation 516 and server 502. Rather, workstation 516 hashes a token provided by token generator 520 with a password to generate a transmission code, and sends that information to server 502. Likewise, server 502 hashes a token provided by token generator 503 with a password to generate a session code, and sends that information to workstation 516. The tokens themselves are not described as being sent between the two locations.

Accordingly, Kaufman et al. fails to disclose all of the elements of claims 1, 4, 8, 13, 15, 16, 21, 24 and 26, and these claims are allowable over Kaufman et al. under the provisions of 35 U.S.C. § 102(b). Claims 2, 5, 6, 9, 10, 14, 17, 18, 22, 23, 25, 27 and 28, which respectively depend from and incorporate the limitations of claims 1, 4, 8, 13, 15, 16, 21, 24 and 26, are also allowable, at least for that reason.

Claim 3, which has been amended into independent form, recites the limitation of a hashing algorithm that includes "hashing the password to derive a first secret" and "hashing the first secret to derive a second secret." Claim 7, which has been amended into independent form, also recites "wherein the key generator hashes the password to derive a first secret" and "hashes the first secret to derive a second secret." Again, Kaufman et al. fails to disclose the concept of hashing a password to derive a first secret, and then hashing the first secret to derive a second secret. Rather, for all the hashing equations described in Kaufman et al., a password is only hashed a second time after it has been concatenated with a token (col. 9:62 – col. 10:17). Performing consecutive hashing operations on the password alone is not disclosed.

Accordingly, Kaufman et al. fails to disclose all of the elements of claims 3 and 7, and these claims are allowable over Kaufman et al. under the provisions of 35 U.S.C. § 102(b).

Claim 11 recites the limitation of "sending an encryption downloadable for deriving a key to encrypt data to the client," and claim 12 recites the limitation of "sending the encryption downloadable to the client." Claim 29 recites "transmitting to a client a hint corresponding to the indication, and a decryption downloadable for deriving an intermediate index from a password and the hint." Claim 30 recites the limitation of "transmitting the decryption downloadable and a hint corresponding to the indication to a client." Kaufman et al. fails to disclose the concept of sending a decryption downloadable to a client.

The Office submits that the transmission code sent by workstation 516 or the encrypted message sent by server 502 are analogous to an encryption downloadable. The transmission code, however, is merely a hashed combination of a numerical token and a password. Moreover, the transmission code is sent from workstation 516 to server 502, and not the other way around. (col. 10:18-21). Likewise, the message sent by server 502 is described as being decrypted by workstation 516 using a session code, and then uses the message as a ticket to gain access to the desired system, or as a shared secret key to encrypt and decrypt subsequent communications with the desired system (col. 11:44-55). Clearly, neither the transmission code nor the encrypted message comprise an encryption downloadable according to the present invention.

Accordingly, Kaufman et al. fails to disclose all of the elements of claims 11, 12, 29 and 30, and these claims are allowable over Kaufman et al. under the provisions of 35 U.S.C. § 102(b).

In view of the foregoing, Applicant respectfully submits that claims 1-18 and 21-30 are allowable over Kaufman et al., and requests that the present rejections be withdrawn.

ENTRY OF AMENDMENTS

The amendments to claims 1, 3, 4, 7, 8, 13, 15, 16, 19 and 20 above should be entered by the Examiner because the amendments are supported by the as-filed specification and drawings and do not add any new matter to the application.

CONCLUSION

Claims 1 through 30 are believed to be in condition for allowance, and an early notice thereof is respectfully solicited. Should the Examiner determine that additional issues remain which might be resolved by a telephone conference, he is respectfully invited to contact Applicant's undersigned attorney.

Respectfully submitted,

Date: April 1, 2005

Greg T. Warder
Registration No. 50,208
MANATT, PHELPS & PHILLIPS LLP
1001 Page Mill Road, Building 2
Palo Alto, California 94304
650-812-1321 Telephone
650-213-0260 Facsimile

20131251.1